UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/653,804	09/01/2000	Laurence Hamid	12-51 US	5986

7590 02/23/2004

Gordon Freedman
Freedman & Associates
Suite 350
117 Centrepointe Drive
Nepean, ON K2G 5X3
CANADA

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 02/23/2004 2

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/653,804	**Applicant(s)** HAMID ET AL.	
	Examiner Kaveh Abrishamkar	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on *01 September 2000*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-44* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on 09/01/2000. Claims 1 – 44 were received for consideration. No preliminary amendments for the claims were filed. Currently claims 1 – 44 are under consideration.

Claim Objections

2. Claim 1 is objected to because of the following informalities: Before the last limitation there should be an "and." Appropriate correction is required.

3. Claims 26 and 42 are objected to because of the following informalities: After the word "useable," the word "from" should be changed to "form." Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 27 – 37, and 39 - 44 are rejected under 35 U.S.C. 102(b) as being anticipated by Lewis (U.S. Patent 5,761,306).

Regarding claim 27, Lewis discloses:

A method of authenticating an individual for allowing access to secure data or secure keys stored on a communication network when other than in communication with a central key-server comprising the steps of:

providing at least a computer in communication with the communication network (Figure 1 item 12, Figure 5 item 12, column 4 lines 30 – 50);

determining at least an available user information entry device from a plurality of known user information entry devices (Figure 1, Figure 5, column 4 lines 30 – 50, column 5 line 25 – column 8 line 10, column 12 lines 12 - 65);

determining the availability of one of a key-server and a portable data storage device in communication with the computer (Figure 1, Figure 5, column 4 lines 30 – 50, column 5 line 25 – column 8 line 10, column 12 lines 12 – 65);

receiving user identification information via the at least an available user information entry device (column 5 line 15 – column 7 line 28); and

authenticating the individual for access to at least one of the secure data and secure keys stored on the determined one of a key-server and a portable data storage device (column 5 line 15 – column 7 line 28).

Claim 28 is rejected as applied above in rejecting claim 27. Furthermore, Lewis discloses:

A method as defined in claim 27 wherein when a portable data storage device is present the determined one of a key-server and a portable data storage device is the portable data storage device and the received user identification information is registered against user identification information stored in the memory means of the portable data storage device (column 5 line 15 – column 7 line 28).

Claim 41 is rejected as applied above in rejecting claim 27. Furthermore, Lewis discloses:

A method as defined in claim 27 wherein the portable data storage device provides dedicated cryptographic functions for the computer using security data stored internal to the portable data storage device (Figure 3, column 3 line 46 – column 4 line 50, column 5 line 25 – column 7 line 54).

Claim 43 is rejected as applied above in rejecting claim 27. Furthermore, Lewis discloses:

A method as defined in claim 27 wherein the key-server provides dedicated cryptographic functions for the computer using security data stored internal to the key-server (Figure 3, column 3 line 46 – column 4 line 50, column 5 line 25 – column 7 line 54).

Claim 29 is rejected as applied above in rejecting claim 28. Furthermore, Lewis discloses:

A method as defined in claim 28 comprising the steps of:

receiving unique user identification information against security data for that user information entry device (column 5 line 15 – column 7 line 28);

registering the received user identification information against security data for that user stored in the portable data storage device (Figure 1 item 12, Figure 5 item 12, column 4 lines 30 – 50); and,

providing secure keys to the user to allow access to encrypted data files that the user has been authenticated to access (column 5 line 15 – column 7 line 28).

Claim 30 is rejected as applied above in rejecting claim 28. Furthermore, Lewis discloses:

A method as defined in claim 28 comprising the steps of:

receiving unique user identification information via the at least an available user information entry device (column 5 line 15 – column 7 line 28);

registering the received user identification information against security data for that user stored in the portable data storage device (Figure 1 item 12, Figure 5 item 12, column 4 lines 30 – 50); and,

providing cryptographic functions within the portable data storage device using the secure keys associated with the authenticated user (column 5 line 15 – column 7 line 28).

Claim 31 is rejected as applied above in rejecting claim 28. Furthermore, Lewis discloses:

A method as defined in claim 28 wherein when a portable data storage device is other than present prompting the user to provide a portable storage device (column 4 lines 30 – 50).

Claim 32 is rejected as applied above in rejecting claim 28. Furthermore, Lewis discloses:

A method as defined in claim 28 wherein other than when the user provides a portable data storage device a key-server in communication with the communication network is the determined one of a key-server and a portable data storage device (Figure 1, Figure 5, column 4 lines 30 – 50, column 5 line 25 – column 8 line 10, column 12 lines 12 – 65).

Claim 42 is rejected as applied above in rejecting claim 41. Furthermore, Lewis discloses:

A method as defined in claim 41 wherein the security data stored internal to the portable data storage device are not accessible in a useable form outside of the key-server and the portable data storage devices (Figure 3, column 3 line 46 – column 4 line 50, column 5 line 25 – column 7 line 54).

Claim 44 is rejected as applied above in rejecting claim 43. Furthermore, Lewis discloses:

A method as defined in claim 43 wherein the security data stored internal to the key-server are not accessible from outside of the key-server and the portable data storage devices (Figure 3, column 3 line 46 – column 4 line 50, column 5 line 25 – column 7 line 54).

.

Claim 33 is rejected as applied above in rejecting claim 32. Furthermore, Lewis discloses:

A method as defined in claim 32 comprising the steps of:

receiving unique user identification information via the at least an available user information entry device (Figure 1, Figure 5, column 4 lines 30 – 50, column 5 line 25 – column 8 line 10, column 12 lines 12 – 65);

registering the received user identification information against security data for that user stored in the key-server (column 5 line 15 – column 7 line 28); and,

providing secure keys to the user to allow access to encrypted data files that the user has been authenticated to access (column 5 line 15 – column 7 line 28).

Claim 34 is rejected as applied above in rejecting claim 32. Furthermore, Lewis discloses:

A method as defined in claim 32 comprising the steps of:

receiving unique user identification information via the at least an available user information entry device (Figure 1, Figure 5, column 4 lines 30 – 50, column 5 line 25 – column 8 line 10, column 12 lines 12 – 65);

registering the received user identification information against security data for that user stored in the key-server (column 5 line 15 – column 7 line 28); and,

providing cryptographic functions within the key-server using the secure keys associated with the authenticated user (column 5 line 15 – column 7 line 28).

Claim 35 is rejected as applied above in rejecting claim 31. Furthermore, Lewis discloses:

A method as defined in claim 31 wherein the portable data storage device is one of a smart card and a PCMCIA token (column 4 lines 43 – 50).

Claim 39 is rejected as applied above in rejecting claim 31. Furthermore, Lewis discloses:

A method as defined in claim 31 wherein a portable data storage device is used to provide an individual with access to a predetermined set of keys in a plurality of different locations (column 4 lines 30 – 54, column 6 line 56 – column 7 line 28).

Claim 36 is rejected as applied above in rejecting claim 35. Furthermore, Lewis discloses:

A method as defined in claim 35 wherein the portable data storage device is in the form of a PCMCIA token provides dedicated cryptographic functions for the computer using security data stored internal to the PCMCIA token (Figure 3, column 3 line 46 – column 4 line 50, column 5 line 25 – column 7 line 54).

Claim 40 is rejected as applied above in rejecting claim 39. Furthermore, Lewis discloses:

A method as defined in claim 39 wherein the method of user authentication required at work is other than the method of user authentication required elsewhere (column 3 line 15 – column 4 line 50).

Claim 37 is rejected as applied above in rejecting claim 36. Furthermore, Lewis discloses:

A method as defined in claim 36 wherein the security data stored internal to the PCMCIA token are not accessible from outside of the PCMCIA token and therefore cannot be extracted or otherwise read by an unauthorized third party (Figure 3, column 3 line 46 – column 4 line 50, column 5 line 25 – column 7 line 54).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis (U.S. Patent 5,761,306) in view of Shen (U.S. Patent 6,611,850).

Regarding claim 1, Lewis discloses:

A key-server in communication with a communication network comprising the steps of:

providing the key-server in communication with the communication network (Figure 1 item 10 and 16, Figure 5 item 10 and 16, column 6 line 23 – column 7 line 38);

providing to at least a computer in communication with the communication network, a plurality of portable data storage devices each having stored thereon security data relating to a single authorized user (Figure 1 item 12, Figure 5 item 12, column 4 lines 30 – 50); and

copying from each of the plurality of portable data storage devices, security data relating to the single authorized user (column 6 line 56 – column 7 line 28).

Lewis does not explicitly state that this method of communicating keys between a key server and a plurality of portable storage devices is for the purpose of restoring the data of the key server. Shen discloses a backup/restore method which data is transferred from a server to a portable storage device (e.g. IC card) for the purpose of providing a system of backup and restoration for the data of the server (column 11 lines 19 – 42). Lewis teaches a communication method of transmitting a plurality of keys for the purpose of redundancy and for the primary purpose of replacing the key based on the possibility of the current keys being compromised, but if additional measures were needed to backup a key server so to prevent loss of data information due to hardware trouble or a computer virus (Shen column 1 lines 16 – 22), the portable storage devices could be used to act as a key restoration process as well, since the replacement keys and current keys are already stored on the portable storage devices and the portable storage devices do communicate with the key server. Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to use the teachings of Lewis in conjunction with the backup/restore process of Shen to provide the additional functionality of the portable storage devices to act as a redundant backup for the key server, in addition to its functionality of storing current and replacement keys. In the case where the key server loses its data (e.g. keys), the portable storage devices of Lewis have the ability to communicate with the key server, and restore the keys with the stored keys.

Regarding claim 14, Lewis discloses:

A key-server in communication with a communication network comprising the steps of:

providing the key-server in communication with the communication network, the key-server having stored thereon the unique user identification information for a plurality of authorized users of the communication network and the security data for use by the specific authorized user in accessing data within the network (Figure 1 item 10, 16, and 24, Figure 5 item 10, 16, and 24, column 6 line 23 – column 7 line 38);

providing to at least a computer in communication with the communication network, a portable data storage device (Figure 1 item 12, Figure 5 item 12, column 4 lines 30 – 50);

receiving user identification data indicative of an authorized user of the communication network (column 5 line 15 – column 7 line 28); and,

copying from the key-server to the portable data storage device, security data relating to the authorized user for use by the specific authorized user in accessing data within the network (column 5 line 15 – column 7 line 28).

Lewis does not explicitly state that this method of communicating keys between a key server and a plurality of portable storage devices is for the purpose of backup up the data of the key server. Shen discloses a backup/restore method which data is transferred from a server to a portable storage device (e.g. IC card) for the purpose of providing a system of backup and restoration for the data of the server (column 11 lines 19 – 42). Lewis teaches a communication method of transmitting a plurality of keys for the purpose of redundancy and for the primary purpose of replacing the key based on the possibility of the current keys being compromised, but if additional measures were needed to backup a key server so to prevent loss of data information due to hardware trouble or a computer virus (Shen column 1 lines 16 – 22), the portable storage devices could be used to act as a key restoration process as well, since the replacement keys and current keys are already stored on the portable storage devices and the portable storage devices do communicate with the key server. Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to use the teachings of Lewis in conjunction with the backup/restore process of Shen to provide the additional functionality of the portable storage devices to act as a redundant backup for the key server, in addition to its functionality of storing current and replacement keys. In the case where the key server loses its data (e.g. keys), the portable storage devices of Lewis have the ability to communicate with the key server, and restore the keys with the stored keys.

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Lewis discloses:

A method of restoring data of a key-server in communication with a communication network as defined in claim 1 wherein the step of copying comprises the steps of:

forming a secure communication session between at least one of the plurality of portable data storage devices and the key-server (Figure 3, column 6 line 56 – column 7 line 28, column 12 lines 21 – 65);

transferring the security data via the secure communication session from the portable data storage device to the key-server (Figure 3, column 6 line 56 – column 7 line 28, column 12 lines 21 – 65); and,

storing the transferred security data within memory means of the key-server (column 6 line 23 – column 7 line 28, column 12 lines 21 – 65).

Claim 15 is rejected as applied above in rejecting claim 14. Furthermore, Lewis discloses:

A method of backing up data of a key-server in communication with a communication network as defined in claim 14 wherein the step of copying comprises the steps of:

forming a secure communication session between the key-server and the portable data storage device (Figure 3, column 6 line 56 – column 7 line 28, column 12 lines 21 – 65);

transferring the security data relating to a specific authorized user via the secure communication session from the key-server to the portable data storage device assigned to that specific authorized user (Figure 3, column 6 line 56 – column 7 line 28, column 12 lines 21 – 65); and,

storing the transferred security data relating to a specific authorized user within the memory means of the portable data storage device (column 6 line 23 – column 7 line 28, column 12 lines 21 – 65).

Claim 3 is rejected as applied above in rejecting claim 2. Furthermore, Lewis discloses:

A key-server in communication with a communication network as defined in claim 2 with a plurality of portable data storage devices. As discussed in the rejection for claim 1, Shen describes a method of restoring the data of a server by using a plurality of storage devices (column 11 lines 19 – 42). Using the same methodology discussed in the rejection for the preceding claims, it is obvious to use the method of transferring keys disclosed by Lewis in conjunction with the restoration procedure discussed by Shen to use portable storage devices to store all of the information in the key server. It is obvious to store all the information in the server on the portable storage devices if it is actually backing up and restoring all the data of the server. Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Lewis and the backup/restoration procedure of Shen to backup all the security data to be restored in the key-server.

Claim 5 is rejected as applied above in rejecting claim 2. Furthermore, Lewis discloses:

A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein the portable data storage device includes a processor for ciphering data using the security data stored therein and comprising the steps of:

providing cryptographic functions within the portable data storage device using the security data stored therein (Figure 3, column 3 line 46 – column 4 line 50, column 5 line 25 – column 7 line 54).

Claim 6 is rejected as applied above in rejecting claim 2. Furthermore, Lewis discloses:

A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein the key-server includes a processor for ciphering data using the security data stored therein and comprising the steps of:

providing cryptographic functions within the key-server using the security data stored therein (Figure 3, column 3 line 46 – column 4 line 50, column 5 line 25 – column 7 line 54).

Claim 10 is rejected as applied above in rejecting claim 2. Furthermore, Lewis discloses:

A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein the portable data storage device is one of a token and a smart card (column 4 lines 43 – 50).

Claim 11 is rejected as applied above in rejecting claim 2. Furthermore, Lewis discloses:

A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein at least a portable data storage device provides dedicated cryptographic functions for the at least a computer in communication with the communication network using the security data stored internal to the at least a portable storage device (Figure 1, Figure 3, column 3 line 46 – column 4 line 50, column 5 line 25 – column 7 line 54).

Claim 13 is rejected as applied above in rejecting claim 2. Furthermore, Lewis discloses:

A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein the key-server provides dedicated cryptographic functions for the at least a computer in communication with the communication network using the security data stored internal to the key-server (Figure 3, column 3 line 46 – column 4 line 50, column 5 line 25 – column 7 line 54).

Claim 16 is rejected as applied above in rejecting claim 15. Furthermore, Lewis discloses:

A method of backing up data of a key-server in communication with a communication network as defined in claim 15 wherein security data specific to each of a plurality of authorized users of the communication network is stored on a separate portable data storage device assigned uniquely to one of the plurality of authorized users (column 6 line 23 – column 7 line 28, column 12 lines 21 – 65). Shen describes a method of restoring the data of a server by using a plurality of storage devices (column 11 lines 19 – 42). Using the same methodology discussed in the rejection for the preceding claims, it is obvious to use the method of transferring keys disclosed by Lewis in conjunction with the restoration procedure discussed by Shen to use portable storage devices to store all of the information in the key server. It is obvious to store all the information in the server on the portable storage devices if it is actually backing up and restoring all the data of the server. Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Lewis and the backup/restoration procedure of Shen to backup all the security data to be restored in the key-server.

Claim 17 is rejected as applied above in rejecting claim 15. Furthermore, Lewis discloses:

A method of backing up data of a key-server in communication with a communication network as defined in claim 15 wherein the portable data storage device includes a processor for ciphering data using the security data stored therein and comprising the steps of:

providing cryptographic functions within the portable data storage using the security data stored therein (Figure 3, column 3 line 46 – column 4 line 50, column 5 line 25 – column 7 line 54).

Claim 18 is rejected as applied above in rejecting claim 15. Furthermore, Lewis discloses:

A method of backing up data of a key-server in communication with a communication network as defined in claim 15 wherein the key-server includes a processor for ciphering data using the security data stored therein and comprising the steps of:

providing cryptographic functions within the key-server using the security data stored therein (Figure 3, column 3 line 46 – column 4 line 50, column 5 line 25 – column 7 line 54).

Claim 23 is rejected as applied above in rejecting claim 15. Furthermore, Lewis discloses:

A method of backing up data of a key-server in communication with a communication network as defined in claim 15 wherein the portable data storage device provides dedicated cryptographic functions for the at least a computer in communication with the communication network using security data stored internal to the portable data storage device (Figure 3, column 3 line 46 – column 4 line 50, column 5 line 25 – column 7 line 54).

Claim 25 is rejected as applied above in rejecting claim 15. Furthermore, Lewis discloses:

A method of backing up data of a key-server in communication with a communication network as defined in claim 15 wherein the key-server provides dedicated cryptographic functions for the at least a computer in communication with the communication network using security data stored internal to the key-server (Figure 3, column 3 line 46 – column 4 line 50, column 5 line 25 – column 7 line 54).

Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Lewis discloses:

A method of restoring data of a key-server in communication with a communication network as defined in claim 3 wherein the plurality of portable data storage devices includes memory having stored therein security data relating to each single authorized user of the communication network (Figure 1 item 12, Figure 5 item 12, column 4 lines 30 – 50).

Claim 7 is rejected as applied above in rejecting claim 6. Furthermore, Lewis discloses:

A method of restoring data of a key-server in communication with a communication network as defined in claim 6 comprising the steps of:

determining at least an available user information entry device from a plurality of known user information entry devices (Figure 1, Figure 5, column 4 lines 30 – 50, column 5 line 25 – column 8 line 10, column 12 lines 12 – 65);

receiving unique user identification information via the at least an available user information entry device (column 5 line 15 – column 7 line 28); and,

registering the received user identification information against security data for that user stored in the key-server (column 5 line 15 – column 7 line 28);

wherein, when the user identification information is indicative of an authorized user the step of ciphering data is performed with security data associated with the authorized user (column 5 line 15 – column 7 line 28).

Claim 8 is rejected as applied above in rejecting claim 3. Furthermore, Lewis discloses:

A method of restoring data of a key-server in communication with a communication network as defined in claim 3 wherein each of the plurality of portable data storage devices are provided at each of a plurality of computers in communication with the network (Figure 1 item 12, Figure 5 item 12, column 4 lines 30 – 50).

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Lewis discloses:

A method of restoring data of a key-server in communication with a communication network as defined in claim 11 wherein the security data stored internal to the at least a portable data storage device are not accessible in a useable form from outside of the key-server and the at least a portable data storage (Figure 3, column 3 line 46 – column 4 line 50, column 5 line 25 – column 7 line 54).

Claim 19 is rejected as applied above in rejecting claim 18. Furthermore, Lewis discloses:

A method of backing up data of a key-server in communication with a communication network as defined in claim 18 comprising the steps of:

determining at least an available user information entry device from a plurality of known user information entry devices (Figure 1, Figure 5, column 4 lines 30 – 50, column 5 line 25 – column 8 line 10, column 12 lines 12 – 65);

receiving unique user identification information via the at least an available user information entry device (column 5 line 15 – column 7 line 28); and,

registering the received user identification information against security data for that user stored in the key-server (column 5 line 15 – column 7 line 28), wherein, when the user identification information is indicative of an authorized user, the step of ciphering data is performed with security data associated with the authorized user (column 5 line 15 – column 7 line 28).

Claim 20 is rejected as applied above in rejecting claim 16. Furthermore, Lewis discloses:

A method of backing up data of a key-server in communication with a communication network as defined in claim 16 wherein each of the plurality of portable data storage devices are provided at each of a plurality of computers in communication with the network (Figure 1 item 12, Figure 5 item 12, column 4 lines 30 – 50).

Claim 22 is rejected as applied above in rejecting claim 16. Furthermore, Lewis discloses:

A method of backing up data of a key-server in communication with a communication network as defined in claim 16 wherein the portable storage device is one of a smart card and a PCMCIA token (column 4 lines 43 – 50).

Claim 24 is rejected as applied above in rejecting claim 23. Furthermore, Lewis discloses:

A method of backing up data of a key-server in communication with a communication network as defined in claim 23 wherein the security data stored internet to the portable data storage device are not accessible from outside of the key-server and the portable data storage device (Figure 3, column 3 line 46 – column 4 line 50, column 5 line 25 – column 7 line 54).

Claim 26 is rejected as applied above in rejecting claim 25. Furthermore, Lewis discloses:

A method of backing up data of a key-server in communication with a communication network as defined in claim 25 wherein the security data stored internal to the key-server are not accessible in a useable form outside of the key-server and the portable data storage device (Figure 3, column 3 line 46 – column 4 line 50, column 5 line 25 – column 7 line 54).

Claim 9 is rejected as applied above in rejecting claim 8. Furthermore, Lewis discloses:

A method of restoring data of a key-server in communication with a communication network as defined in claim 8 wherein the portable data storage device is one of a token and a smart card (column 4 lines 43 – 50).

Claim 21 is rejected as applied above in rejecting claim 20. Furthermore, Lewis discloses:

A method of backing up data of a key-server in communication with a communication network as defined in claim 20 wherein the portable storage device is one of a smart card and a PCMCIA token (column 4 lines 43 – 50).

6. Claim 38 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis (U.S. Patent 5,761,306) in view of Burger (U.S. Patent 6,611,850).

Claim 38 is rejected as applied above in rejecting claim 32. Lewis does not explicitly describe a method as defined in claim 32 wherein the user information entry device is a biometric device. Burger discloses a biometric authentication system which includes an input reader which can read biometric information and compare it to information disposed on a smart card for authentication purposes. Lewis teaches the use of a smart card for receiving and storing keys. Authentication can be also received from comparing the user's keys to the stored keys, but the biometric authentication method discloses by Burger would add another measure of security which is more user specific than a key pair. Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to use the biometric input mechanism disclosed by Burger in conjunction with the teachings of Lewis to add an additional measure of authentication when accessing a network and the keys associated with the users.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 703-305-8892. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

KA
02/17/04

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100